Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Combinatorial Theory, Series A 107 (2004) 49–67
Journal of Combinatorial Theory Series A
http://www.elsevier.com/locate/jcta

Olson's constant for the group $\mathbb{Z}_p \oplus \mathbb{Z}_p$

W.D. Gao,[a] I.Z. Ruzsa,[b] and R. Thangadurai[c]

[a] *Department of Computer Science and Technology, University of Petroleum, Changping Shuiku Road, Beijing, 102200, China*
[b] *Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences, Budapest, Pf. 127, H-1364, Hungary*
[c] *School of Mathematics, Harish Chandra Research Institute, Chhatnag Road, Jhusi, Allahabad 211019, India*

Received 18 May 2003

Abstract

Let G be a finite abelian group. By $Ol(G)$, we mean the smallest integer t such that every subset $A \subset G$ of cardinality t contains a non-empty subset whose sum is zero. In this article, we shall prove that for all primes $p > 4.67 \times 10^{34}$, we have $Ol(\mathbb{Z}_p \oplus \mathbb{Z}_p) = p + Ol(\mathbb{Z}_p) - 1$ and hence we have $Ol(\mathbb{Z}_p \oplus \mathbb{Z}_p) \leqslant p - 1 + \lceil \sqrt{2p} + 5 \log p \rceil$. This, in particular, proves that a conjecture of Erdős (stated below) is true for the group $\mathbb{Z}_p \oplus \mathbb{Z}_p$ for all primes $p > 4.67 \times 10^{34}$.

1. Introduction

Let G be a finite abelian group (written additively). Then $G = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_r}$ with $1 < n_1 | n_2 | \cdots | n_r$, where $n_r = \exp(G) \coloneqq n$ is the exponent of G and where r is the rank of G. When $n_1 = n_2 = \cdots = n_r = n$, then we denote the group $\underbrace{\mathbb{Z}_n \oplus \mathbb{Z}_n \oplus \cdots \oplus \mathbb{Z}_n}_{r \text{ times}}$ by $\mathbb{Z}_n^r$.

Definition 1. By $Ol(G)$ we denote the smallest positive integer t such that every subset of G of cardinality t contains a non-empty subset whose sum is the identity element of G.

E-mail addresses: wdgao@public.fhnet.cn.net (W.D. Gao), ruzsa@renyi.hu (I.Z. Ruzsa), thanga@mri.ernet.in (R. Thangadurai).

0097-3165/$ - see front matter
doi:10.1016/j.jcta.2004.03.007

This constant, $Ol(G)$, is called Olson's constant. Indeed, $Ol(G)$ is the analog of $D(G)$ (Davenport Constant) with no repetitions of elements of G. The name of this constant was proposed in 1994, during a seminar held at *Universidad Central de Venezuela* (Caracas), (see [12]) as a tribute to Olson and his work on this subject.

One of the first results on this constant is due to Szemerédi [16], who proved a conjecture of Erdős and Heilbronn [8], namely that there exists a constant c such that $Ol(G) \leqslant c\sqrt{n}$ where $|G| = n$.

Conjecture 1 (Erdős and Graham [7]). *If G is an abelian group of order n, then $Ol(G) \leqslant \sqrt{2n}$.*

First, let us note that $Ol(\mathbb{Z}_n^2) \geqslant n + Ol(\mathbb{Z}_n) - 1$. For, let $\{a_1, a_2, \ldots, a_{Ol(\mathbb{Z}_n)-1}\}$ be a subset of $\mathbb{Z}_n$ such that it contains no non-empty subset whose sum is zero (by definition of $Ol(\mathbb{Z}_n)$). Consider the following subset:

$$S = \{(1,0), (1,1), \ldots, (1, n-2), (0, a_1), (0, a_2), \ldots, (0, a_{Ol(\mathbb{Z}_n)-1})\}$$

Then $|S| = n + Ol(\mathbb{Z}_n) - 2$ and clearly, S contains no non-empty subset whose sum is zero in $\mathbb{Z}_n^2$. Therefore, $Ol(\mathbb{Z}_n^2) > |S| = n + Ol(\mathbb{Z}_n) - 2$.

Throughout this paper, let p always denote a prime. First Olson [13,14] showed that $Ol(G) \leqslant 3\sqrt{n}$ (here $n = |G|$) and that $Ol(\mathbb{Z}_p) \leqslant 2\sqrt{p}$. Best known result is due to Hamidoune and Zémor [11] and they show that $Ol(\mathbb{Z}_p) \leqslant \lceil \sqrt{2p} + 5 \log p \rceil$ and that $Ol(G) \leqslant \lceil \sqrt{2n} + \gamma(n) \rceil$, where $n = |G|$ and $\gamma(n) = O(n^{1/3} \log n)$. More recently, Julio C. Subocz G [12] proved that $Ol(\mathbb{Z}_2^n) = n + 1$ and $Ol(\mathbb{Z}_3^n) = 2n + 1$ for $n \geqslant 3$. In addition, he had supplied a table with the values of $Ol(G)$ for all abelian groups G with orders $\leqslant 55$.

In this paper, our main result is as follows.

Theorem 1.1. *For any prime number $p > 4.67 \times 10^{34}$, we have*

$$Ol(\mathbb{Z}_p^2) = p + Ol(\mathbb{Z}_p) - 1$$

and hence $Ol(\mathbb{Z}_p^2) \leqslant p - 1 + \lceil \sqrt{2p} + 5 \log p \rceil$. In particular, Conjecture 1 is true for the group $G = \mathbb{Z}_p \oplus \mathbb{Z}_p$ for all primes $p > 4.67 \times 10^{34}$.

Conjecture 2. *For any integer $n \geqslant 3$, and $k \geqslant 2$ we have*

$$Ol(\mathbb{Z}_n^k) = n + Ol(\mathbb{Z}_n^{k-1}) - 1.$$

By a result of [10, Corollary 7.4] we know that $Ol(\mathbb{Z}_p^k) = D(\mathbb{Z}_p^k) = k(p-1) + 1$ provided that $k \geqslant 2p + 1$. Hence, Conjecture 2 holds for the case that $k \geqslant 2p + 1$.

Before we discuss further, we shall introduce notations once for all. By a sequence S in G of length l, we mean a multi-set of G with cardinality (counting multiplicities) l. We also denote this cardinality by $|S|$. For convenience, we write any sequence S in G of length l as $S = \prod_{i=1}^{l} g_i$. Also, $v_g(S)$ denotes the number of times g appears in S. Let $\sigma(S) = \sum_{i=1}^{l} g_i$. We denote any subsequence T of S by $T \mid S$. Also, if T is a subsequence of S, then the deleted sequence ST^{-1} is the sequence obtained by removing from S the elements in T. Let $\mathrm{Supp}(S)$ be the set that consists of all distinct elements in S. We say that the sequence $S = \prod_{i=1}^{l} g_i$ in G is

- a zero sequence, if $\sigma(S) = 0$ in G. (We do not regard the empty sequence as a zero sequence).
- a zero-free sequence, if none of its subsequences is a zero sequence.

For every $1 \leqslant k \leqslant l$, define

$$\sum_k (S) = \{g_{i_1} + g_{i_2} + \cdots + g_{i_k}\colon\ 1 \leqslant i_1 < \cdots < i_k \leqslant l\}$$

and define

$$\sum (S) = \{g_{i_1} + g_{i_2} + \cdots + g_{i_s}\colon\ 1 \leqslant i_1 < \cdots < i_s \leqslant l, 1 \leqslant s \leqslant l\}.$$

Clearly, $\sum(S) = \bigcup_{k=1}^{l} \sum_k(S)$.

If $S = \prod_{i=1}^{p+Ol(\mathbb{Z}_p)-1} (a_i, b_i)$ is a sequence in $\mathbb{Z}_p^2$, then $\pi_1(S) = \prod_{i=1}^{p+Ol(\mathbb{Z}_p)-1} a_i$ (respectively, $\pi_2(S) = \prod_{i=1}^{p+Ol(\mathbb{Z}_p)-1} b_i$) is the sequence in $\mathbb{Z}_p$ where the elements a_i (respectively, b_i) are simply the first (respectively, second) co-ordinates of S. We call $\pi_1(S)$ (respectively, $\pi_2(S)$) as the first (respectively, second) co-ordinate sequence of S. One can write $\pi_1(S)$ in the following form:

$$\pi_1(S) = x_1^{m_1} x_2^{m_2} \cdots x_r^{m_r} y_1^2 y_2^2 \cdots y_u^2 z_1 z_2 \cdots z_v,$$

where $x_1, x_2, \ldots, x_r, y_1, y_2, \ldots, y_u, z_1, z_2, \ldots, z_v$ are pairwise distinct elements in $\mathbb{Z}_p$, $r, u, v \geqslant 0$, $m_1, m_2, \ldots, m_r \geqslant 3$ are integers and $m_1 + m_2 + \cdots + m_r + 2u + v = p + Ol(\mathbb{Z}_p) - 1$. Throughout this article, we shall freely use these constants r, u, v without mentioning.

Also, for any subsequence $R | \pi_1(S)$, we define the following;

$$h = h(R) := \max\{v_g(R)\colon\ g \in \mathbb{Z}_p\}.$$

In other words, h denotes the maximum number of times that an element appears in R. In order to follow the same notation, we write subsets also in the product form as we write for sequences and zero-sum subsets correspond to zero subsequences.

2. Preliminaries

In this section, we shall work-out some preliminaries for our main result.

Theorem 2.1 (Dias da Silva and Hamidoune [6], Alon et al. [2]). *If A is a non-empty subset of $\mathbb{Z}_p$ and if $1 \leqslant k \leqslant |A|$, then*

$$\left|\sum_k (A)\right| \geqslant \min\{p, k(|A| - k) + 1\}.$$

Theorem 2.2 (Dias da Silva and Hamidoune [6]). *Let $p > 3$ be a prime. Let $k = [\sqrt{4p-7}] + 1$ and $l = [k/2]$. Let S be a subset of $\mathbb{Z}_p$ of cardinality k. Then $\sum_l(S) = \mathbb{Z}_p$*

Theorem 2.3 (Cauchy–Davenport Inequality, [4,5]). *If $A_1, A_2, \ldots, A_l$ are non-empty subsets of $\mathbb{Z}_p$, then*

$$|A_1 + A_2 + \cdots + A_l| \geqslant \min\left\{p, \sum_{i=1}^{l} |A_i| - l + 1\right\}.$$

The following technical theorem is very crucial for our main result.

Theorem 2.4. *Let*

$$S = \prod_{i=1}^{l} (a_i, b_1^{(i)}) \cdots (a_i, b_{n_i}^{(i)})$$

be a subset of cardinality $n_1 + \cdots + n_l = p + Ol(\mathbb{Z}_p) - 1$ in $\mathbb{Z}_p^2$ and $a_1, a_2, \ldots, a_l$ are pairwise distinct. Let $W = \prod_{i=1}^{l} a_i^{w_i}$ be a zero subsequence of $\pi_1(S)$, where $0 \leqslant w_i \leqslant n_i$ for each $i = 1, 2, \ldots, l$. If $1 + \sum_{i=1}^{l} w_i(n_i - w_i) \geqslant p$, then S contains a zero-sum subset.

Proof. Since S is a subset of $\mathbb{Z}_p^2$, for every $i \in \{1, 2, \ldots, l\}$, we have $b_1^{(i)}, \ldots, b_{n_i}^{(i)}$ are pairwise distinct in $\mathbb{Z}_p$. Set $B_i = \{b_1^{(i)}, b_2^{(i)}, \ldots, b_{n_i}^{(i)}\}$ for every $i = 1, 2, \ldots, l$. Then it suffices to prove that

$$0 \in \sum_{w_1} (B_1) + \sum_{w_2} (B_2) + \cdots + \sum_{w_l} (B_l).$$

By Theorem 2.1, we see that for each i, we have

$$\left|\sum_{w_i} (B_i)\right| \geqslant \min\{p, w_i(n_i - w_i) + 1\}. \tag{1}$$

Therefore, by Theorem 2.3, we have

$$\left|\sum_{w_1} (B_1) + \sum_{w_2} (B_2) + \cdots + \sum_{w_l} (B_l)\right| \geqslant \min\left\{p, \left|\sum_{w_1}(B_1)\right| + \cdots + \left|\sum_{w_l}(B_l)\right| - l + 1\right\}.$$

Therefore by (1), the left-hand side is at least

$$\begin{aligned} &\geqslant \min\{p, (w_1(n_1 - w_1) + 1) + \cdots + (w_l(n_l - w_l) + 1) - l + 1\} \\ &= \min\{p, w_1(n_1 - w_1) + \cdots + w_l(n_l - w_l) + 1\} \\ &= p. \end{aligned}$$

Therefore we have

$$\sum_{w_1} (B_1) + \cdots + \sum_{w_l}(B_l) = \mathbb{Z}_p \Rightarrow 0 \in \sum_{w_1} (B_1) + \cdots + \sum_{w_l} (B_l).$$

Thus the theorem follows. $\square$

Theorem 2.5. (1) *If A, B are finite subsets of G, such that $0 \in A \cap B$, and $0 = a + b, a \in A, b \in B$ implies $a = 0 = b$, then $|A + B| \geqslant |A| + |B| - 1$.* [15,3]

(2) *Let S be a zero-free sequence in G, and let $S_1, S_2, \ldots, S_r$ be disjoint subsequences of S. Then*

$$\left|\sum(S)\right| \geqslant \sum_{i=1}^{r} \left|\sum(S_i)\right|.$$

Proof of (2). Set $A_i = \{0\} \cup (\sum(S_i))$ for $i = 1, \ldots, r$. Then $(A_1 + A_2 + \cdots + A_r)\backslash\{0\} \subset \sum(S)$. It follows from (1) that $|\sum(S)| \geqslant |A_1 + \cdots + A_r| - 1 = |(A_1 + \cdots + A_{r-1}) + A_r| - 1 \geqslant |A_1 + \cdots + A_{r-1}| + |A_r| - 2 \geqslant \cdots \geqslant |A_1| + |A_2| + \cdots + |A_r| - r = \sum_{i=1}^{r} |\sum(S_i)|$. $\square$

Definition 2. Let G be a finite abelian group. For every integer $k \geqslant 1$, we define

$$f(G, k) = \min\left\{\left|\sum(S)\right| : S \text{ is a zero-free subset of } G \text{ with } |S| = k\right\},$$

and set $f(G, k) = \infty$ if there is no subset of G of the above form.

Theorem 2.6 (Gao and Geroldinger [9]). *Let $n \geqslant 4$ be an integer. Let S be a zero-free sequence in $\mathbb{Z}_n$. Then there exists an element $g \in \mathbb{Z}_n$ such that*

$$v_g(S) \geqslant \frac{1}{k-1}\left(|S| - \frac{n-k-1}{f(\mathbb{Z}_n, k)}\right) \textit{ whenever } |S| \geqslant \left(\frac{n-k}{f(\mathbb{Z}_n, k)} + 1\right)k.$$

Theorem 2.7. *Let p be a prime and k be an integer such that $2 \leqslant k \leqslant Ol(\mathbb{Z}_p) - 1$. Let S be a zero-free sequence in $\mathbb{Z}_p$ of length $|S| \geqslant 4k(p-k)/(k^2+3) + k$. Then there exists an element $g \in \mathbb{Z}_p$ such that*

$$v_g(S) \geqslant \frac{1}{k-1}\left(|S| - \frac{4(p-k-1)}{k^2+3}\right).$$

Proof. Set $l = [\frac{k}{2}]$. Then by Theorem 2.1, we have

$$f(\mathbb{Z}_p, k) \geqslant l(k-l) + 1 \geqslant \frac{k^2+3}{4}.$$

Since $|S| \geqslant \frac{4k(p-k)}{k^2+3} + k \geqslant \left(\frac{p-k}{f(\mathbb{Z}_p,k)} + 1\right)k$, the result follows by Theorem 2.6. $\square$

Theorem 2.8. *Let p be a prime, and q an integer with $2 \leqslant q \leqslant p-1$. Let $Q = \prod_{i=1}^{q} a_i$ be a sequence in $\mathbb{Z}_p\backslash\{0\}$. If $|\sum(Q)\backslash\{0\}| \leqslant q$, then $Q = b^{\alpha}(-b)^{q-\alpha}$ for some $0 \neq b \in \mathbb{Z}_p$, where $q/2 \leqslant \alpha \leqslant q$.*

Proof. Clearly, it suffices to prove that $a_i \in \{a_1, -a_1\}$ for every $i = 2, \ldots, q$. Assume to the contrary that $a_i \neq a_1, -a_1$ for some $i \in \{2, 3, \ldots, q\}$. Without loss of generality we may assume that $i = 2$. Then the elements $0, a_1, a_2, a_1 + a_2$ are pairwise distinct.

Now by Theorem 2.3, we infer that

$$\begin{aligned}\left|\sum(Q)\backslash\{0\}\right| &= |(\{0,a_1\}+\{0,a_2\}+\cdots+\{0,a_q\})\backslash\{0\}|\\ &= |(\{0,a_1,a_2,a_1+a_2\}+\{0,a_3\}+\cdots+\{0,a_q\})\backslash\{0\}|\\ &\geqslant \min\{p, 4+2(q-2)-(q-2)-1\} = q+1,\end{aligned}$$

a contradiction. □

Theorem 2.9 (Bovey et al. [3]). *Let n, k be two positive integers satisfying $n-2k\geqslant 1$. Let S be a zero-free sequence in $\mathbb{Z}_n$ of length $n-k$. Then there exists an element $a\in\mathbb{Z}_n$ such that $v_a(S)\geqslant n-2k+1$.*

3. Proof of Theorem 1.1

Lemma 3.2. *Let p be any odd prime. Let $S=\prod_{i=1}^{p+Ol(\mathbb{Z}_p)-1}(a_i,b_i)$ be a subset of $\mathbb{Z}_p^2$ of cardinality $p+Ol(\mathbb{Z}_p)-1$. If $h(\pi_1(S))\geqslant p$, then S contains a zero-sum subset.*

Proof. Without loss of generality, we assume that $a_1=a_2=\cdots=a_p$. Since S is subset of $\mathbb{Z}_p^2$, the sequence $b_1,b_2,\dots,b_p$ runs through every residue classes modulo p. Hence $b_1+b_2+\cdots+b_p=0$ in $\mathbb{Z}_p$. Thus $\prod_{i=1}^{p}(a_i,b_i)$ is a zero-sum subset of S. □

Remark 3.3. (i) From the above lemma, it is enough to assume that $h(\pi_1(S))\leqslant p-1$, and from now to Theorem 3.9 (except in Lemma 3.7) we always assume that $h(\pi_1(S))\geqslant Ol(\mathbb{Z}_p)$.

(ii) Let $S=\prod_{i=1}^{p+Ol(\mathbb{Z}_p)-1}(a_i,b_i)$ be a subset of $\mathbb{Z}_p^2$ of cardinality $p+Ol(\mathbb{Z}_p)-1$. If 0 occurs at least $Ol(\mathbb{Z}_p)$ times in the sequence $\prod_{i=1}^{p+Ol(\mathbb{Z}_p)-1}a_i$ (similarly in $\prod_{i=1}^{p+Ol(\mathbb{Z}_p)-1}b_i$), then by the definition of $Ol(\mathbb{Z}_p)$, S contains a non-empty zero-sum subset. So, we may always assume that 0 occurs at most $Ol(\mathbb{Z}_p)-1$ times both in $\prod_{i=1}^{p+Ol(\mathbb{Z}_p)-1}a_i$ and $\prod_{i=1}^{p+Ol(\mathbb{Z}_p)-1}b_i$. Therefore, if some element a occurs at least $Ol(\mathbb{Z}_p)$ times in $\prod_{i=1}^{p+Ol(\mathbb{Z}_p)-1}a_i$ or $\prod_{i=1}^{p+Ol(\mathbb{Z}_p)-1}b_i$, we always assume that $a\neq 0$.

Without loss of generality we can assume that 1 is repeated $h=h(\pi_1(S))$ times. Thus, by rearranging if necessary, we have

$$\pi_1(S)=0^{d-\ell-1}1^hQ,$$

where $0\leqslant\ell\leqslant d-1$, $d=Ol(\mathbb{Z}_p)$, and $Q=\prod_{i=1}^{p-h+\ell}a_i$ is a sequence of length $p-h+\ell$ with $a_i\in\mathbb{Z}_p\backslash\{0,1\}$.

It is clear that

$$\sum(Q)\backslash\{0\}=(\{0,a_1\}+\{0,a_2\}+\cdots+\{0,a_{p-h+\ell}\})\backslash\{0\}.$$

Therefore, by Theorem 2.3, we have

$$\left|\sum(Q)\backslash\{0\}\right| \geqslant p-h+\ell. \tag{2}$$

Lemma 3.4. *Let $p \geqslant 367$ be any prime number. Let $S=\prod_{i=1}^{p+d-1}(a_i,b_i)$ be a subset of $\mathbb{Z}_p^2$. If $h=h(\pi_1(S))$ satisfies $\frac{2p}{3} \leqslant h < p$, then S contains a zero-sum subset.*

Proof. We distinguish three cases.

Case 1: ($\ell \geqslant 3$). By (2), we have $|\sum(Q)\backslash\{0\}| \geqslant p-h+3$. Therefore, $|\sum(Q)\backslash\{0\}| + |\{p-h+2, p-h+3, \ldots, p-2\}| \geqslant p-h+3+(h-3)=p>|\mathbb{Z}_p\backslash\{0\}|$. Hence, $(\sum(Q)\backslash\{0\}) \cap \{p-h+2, p-h+3, \ldots, p-2\} \neq \emptyset$, i.e., there is a non-empty subset $I \subset \{1, 2, \ldots, p-h+\ell\}$ such that

$$\sum_{i \in I} a_i \in \{p-h+2, p-h+3, \ldots, p-2\}.$$

Now consider the following sequence:

$$W = 1^{p-\sum_{i\in I} a_i} \prod_{i \in I} a_i,$$

which is a zero subsequence of $\pi_1(S)$. Since $p-\sum_{i\in I} a_i \in \{2, 3, \ldots, h-2\}$, we have

$$\left(p-\sum_{i\in I} a_i\right)\left(h-\left(p-\sum_{i\in I} a_i\right)\right)+1 \geqslant 2(h-2)+1 \geqslant p.$$

Therefore, by Theorem 2.4, the result follows.

Case 2: ($1 \leqslant \ell \leqslant 2$). Set $t=\left[\frac{d-1-\ell}{2}\right]$. By (2), we have $|\sum(Q)\backslash\{0\}| \geqslant p-h+1$. Therefore, there is a non-empty subset $I \subset \{1, 2, \ldots, p-h+\ell\}$ such that

$$\sum_{i\in I} a_i \in \{p-h+1, p-h+2, \ldots, p-1\}.$$

Therefore, we have $p-\sum_{i\in I} a_i \in \{1, 2, \ldots, h-1\}$. Now consider the sequence

$$W = 0^t 1^{p-\sum_{i\in I} a_i} \prod_{i\in I} a_i,$$

which is a zero subsequence of $\pi_1(S)$. Since

$$\begin{aligned} t(d-1-\ell-t)+(h-1)+1 &\geqslant \frac{2p}{3}+\frac{(d-1-\ell)^2-1}{4} \\ &\geqslant \frac{2p}{3}+\frac{([\sqrt{2p}-1]-3)^2-1}{4} \geqslant p, \end{aligned}$$

by Theorem 2.4 the result follows.

Case 3: ($\ell=0$) If $|\sum(Q)\backslash\{0\}| \geqslant p-h+1$, then in a similar way to Case 2, we can get the result. So, we may assume that $|\sum(Q)\backslash\{0\}|=p-h$. Then by Theorem 2.8, it follows that $Q=b^{\alpha}(-b)^{p-h-\alpha}$ for some $b \in \mathbb{Z}_p\backslash\{0,1\}$, where $\frac{p-h}{2} \leqslant \alpha \leqslant p-h$. If $\alpha = p-h$, then by Theorem 2.9, we have $1^{h-1}b^{p-h}$ contains a non-empty zero subsequence, say, R. Clearly, $R = 1^m b^n$ with $1 \leqslant m \leqslant h-1$ and $1 \leqslant n \leqslant p-h$. By setting, $t = \left[\frac{d-1}{2}\right]$ and $W = R0^t$, we see that the result follows in similar way to Case 2. So we may assume that $\alpha \leqslant p-h-1$. Since $2p/3 < h \leqslant p-1$, either $1 \leqslant p-b \leqslant h-1$ or $b \leqslant h-1$. If $p-b \leqslant h-1$, then $1^{p-b}b$ is a zero subsequence of $1^{h-1}b^{\alpha}$ and by setting $t = \left[\frac{d-1}{2}\right]$ and $W = 1^{p-b}b0^t$, we can proceed to prove the result similar to Case 2. If $b \leqslant h-1$, then $1^b(-b)$ is a zero subsequence of $1^{h-1}(-b)^{p-h-\alpha}$. Setting $t = \left[\frac{d-1}{2}\right]$ and $W = 1^b(-b)0^t$, then we prove the result similar to the proof of Case 2. $\square$

Lemma 3.5. *Let $p > 838$ be any prime number and let $S = \prod_{i=1}^{p+d-1}(a_i, b_i)$ be a subset of $\mathbb{Z}_p^2$ of cardinality $p+d-1$. If $h = h(\pi_1(S))$ satisfying $\frac{2p}{5} \leqslant h < \frac{2p}{3}$, then S contains a zero-sum subset.*

Proof. Recall that $d = Ol(\mathbb{Z}_p)$. We know, by the result in [11], that $d \leqslant \sqrt{2p} + 5\log p$. Since $p > 838$, we infer that, $p > 15(\sqrt{2p} + 5\log p) > 15d$. Hence, $p \geqslant 15d+1$. We distinguish five cases.

Case 1: ($\ell \geqslant 5$). By (2), we have $|\sum(Q)\backslash\{0\}| \geqslant p-h+5$. Therefore, there is a non-empty subset $I \subset \{1, 2, \ldots, p-h+\ell\}$ such that

$$\sum_{i \in I} a_i \in \{p-h+3, p-h+4, \ldots, p-3\}.$$

Now consider the sequence

$$W = 1^{p-\sum_{i\in I} a_i} \prod_{i \in I} a_i,$$

which is a zero subsequence of $\pi_1(S)$. Since

$$\left(p - \sum_{i \in I} a_i\right)\left(h - \left(p - \sum_{i \in I} a_i\right)\right) + 1 \geqslant 3(h-3) + 1 \geqslant p,$$

the result follows from Theorem 2.4.

Case 2: ($3 \leqslant \ell \leqslant 4$). Set $t = \left[\frac{d-1-\ell}{2}\right]$. By (2), we have $|\sum(Q)\backslash\{0\}| \geqslant p-h+3$. Therefore, there is a non-empty subset $I \subset \{1, 2, \ldots, p-h+\ell\}$ such that

$$\sum_{i \in I} a_i \in \{p-h+2, p-h+3, \ldots, p-2\}.$$

Now consider the sequence

$$W = 0^t 1^{p-\sum_{i\in I} a_i} \prod_{i \in I} a_i,$$

which is a zero subsequence of $\pi_1(S)$. Since

$$2(h-2)+t(d-1-\ell-t)\geqslant 2\left(\frac{2p}{5}-2\right)+\frac{(d-1-\ell)^2-1}{4}$$
$$\geqslant \frac{4(p-5)}{5}+\frac{([\sqrt{2p}-1]-5)^2-1}{4}\geqslant p,$$

the result follows from Theorem 2.4.

Case 3: ($\ell=2$). If $|\sum(Q)\backslash\{0\}|\geqslant p-h+3$, then the result follows by Case 2. So, we may assume that $|\sum(Q)\backslash\{0\}|=p-h+2$. By Theorem 2.8, it follows that $Q=b^{\alpha}(-b)^{p-h+2-\alpha}$ for some $b\in\mathbb{Z}_p\backslash\{0,1\}$, where $\frac{p-h+2}{2}\leqslant\alpha\leqslant p-h+2$. If $\alpha\leqslant p-h-2=(p-h+2)-4$, then $W=b^4(-b)^4$ is a zero subsequence of Q. Since $4(\alpha-4)+4(p-h+2-\alpha-4)+1=4(p-h-6)+1\geqslant 4(p/3-6)+1\geqslant p$, by Theorem 2.4 we get the result. So we can assume that $p-h-1\leqslant\alpha\leqslant p-h+2$. Consider the subsequence $1^{h-1}b^{p-h-2}$ of the sequence $1^{h-1}b^{\alpha-1}$. Since $2p/5\leqslant h<2p/3$, we infer that, $p-2\times 3+1=p-5>\max\{h-1,p-h-2\}$. It follows from Theorem 2.9 that, $1^{h-1}b^{p-h-2}$ contains a zero subsequence of the form $1^m b^n$ with $1\leqslant m\leqslant h-1$ and $1\leqslant n\leqslant p-h-2\leqslant\alpha-1$. Set $t=[\frac{d-3}{2}]$ and $W=0^t1^mb^n$. Now since, $m(h-m)+n(\alpha-n)+t(d-3-t)+1\geqslant(h-1)+(\alpha-1)+t(d-3-t)+1\geqslant p-1+t(d-3-t)+1>p$, once again the result follows from Theorem 2.4.

Case 4: ($\ell=1$). By (2), we have $|\sum(Q)\backslash\{0\}|\geqslant p-h+1$. Therefore, there is a non-empty subset $I\subset\{1,2,\dots,p-h+1\}$ such that $\sum_{i\in I}a_i\in\{p-h+1,p-h+2,\dots,p-1\}$. In this case, the sequence is

$$S=\prod_{i=1}^{p-h+1}(a_i,b_i)\prod_{i=p-h+2}^{p-h+d-1}(0,b_i)\prod_{i=p-h+d}^{p+d-1}(1,b_i).$$

Now consider the sequence

$$W=1^{p-\sum_{i\in I}a_i}\prod_{i\in I}a_i,$$

which is a zero subsequence of $\pi_1(S)$. Put $q=p-\sum_{i\in I}a_i$ and hence $q\in\{1,2,\dots,h-1\}$. Since $a_i=1$ for all $i\in\{p+d-h,p+d-h+1,\dots,p+d-1\}$, the corresponding second co-ordinates b_i's are pairwise distinct. Let

$$A'=\{b_{p+d-h},b_{p+d-h+1},\dots,b_{p+d-1}\}.$$

Then by letting

$$A=\sum_{i\in I}b_i+\sum_q(A')=\left\{\sum_{i\in I}b_i+\beta:\beta\in\sum_q(A')\right\},$$

and recalling that $p\geqslant 15d+1$ we see that

$$|A|\geqslant h>\frac{2p}{5}>\frac{p}{3}+2+(d-2).$$

Setting

$$B = A\backslash\{b_{p-h+2}, b_{p-h+3}, \ldots, b_{p-h+d-1}\}, \text{ we have } |B| \geqslant \frac{p}{3} + 2.$$

It follows from Theorem 2.1 that

$$\left|\sum_{2}(B)\right| \geqslant 2\left(\frac{p}{3} + 2 - 2\right) + 1 = \frac{2p}{3} + 1.$$

Therefore, $B \cap \sum_2(B) \neq \emptyset$. That is, there are two distinct elements $c_1, c_2 \in B$ such that $c_1 + c_2 \in B$. By the definition of B, there are two subsequences S_1 and S_2 of S such that the first co-ordinate sequences of S_1 as well as S_2 are of the form $1^{p-\sum_{i\in I} a_i} \prod_{i\in I} a_i$, and such that $\sigma(S_1) = (0, c_1)$ and $\sigma(S_2) = (0, c_2)$. Set $U = (0, c_1)(0, c_2) \prod_{i=p-h+2}^{p-h+d-1} (0, b_i)$. Since $c_1 + c_2 \in B$, we have $\sum(U) \subset \sum(S)$. But $|U| = d = Ol(\mathbb{Z}_p)$, by the definition of $Ol(\mathbb{Z}_p)$, we see that $(0,0) \in \sum(U) \subset \sum(S)$.

Case 5: ($\ell = 0$). If $|\sum(Q)\backslash\{0\}| \geqslant p - h + 1$, then similar to the proof of Case 4, one can prove the theorem. So, we may assume that $|\sum(Q)\backslash\{0\}| = p - h$. Therefore, by Theorem 2.8, we see that $Q = b^{\alpha}(-b)^{p-h-\alpha}$ for some $b \in \mathbb{Z}_p\backslash\{0,1\}$, where $\frac{p-h}{2} \leqslant \alpha \leqslant p - h$. Thus we get the result in a similar way to the proof of Case 3. $\square$

Lemma 3.6. *Let $p > 5 \times 10^7$ be any prime number. Let $S = \prod_{i=1}^{p+d-1}(a_i, b_i)$ be a subset of $\mathbb{Z}_p^2$. If $h = h(\pi_1(S))$ satisfies $\frac{p}{360} \leqslant h < \frac{2p}{5}$, then S contains a zero-sum subset.*

Proof. We distinguish two cases.

Case 1: ($\ell \geqslant 721$). By (2), we have $|\sum(Q)\backslash\{0\}| \geqslant p - h + 721$. Therefore, there is a non-empty subset $I \subset \{1, 2, \ldots, p - h + \ell\}$ such that $\sum_{i\in I} a_i \in \{p - h + 361, p - h + 362, \ldots, p - 361\}$. Now consider the sequence

$$W = 1^{p-\sum_{i\in I} a_i} \prod_{i\in I} a_i$$

which is a zero subsequence of $\pi_1(S)$. Since $p - \sum_{i\in I} a_i \in \{361, 362, \ldots, h - 361\}$ and $p > 5 \times 10^7$ we have

$$\left(p - \sum_{i\in I} a_i\right)\left(h - \left(p - \sum_{i\in I} a_i\right)\right) + 1 \geqslant 361(h - 361) + 1 \geqslant p.$$

Therefore, by Theorem 2.4, the result follows.

Case 2: ($0 \leqslant \ell \leqslant 720$). If $|\sum(Q)\backslash\{0\}| \geqslant p - h + 721$, then similar to the proof of Case 1, one can get the result. So, we may assume that $|\sum(Q)\backslash\{0\}| \leqslant p - h + 720$. Let t be the largest integer such that there are t disjoint subsequences $\{c_1, d_1\}, \{c_2, d_2\}, \ldots, \{c_t, d_t\}$ of $Q = \prod_{i=1}^{p-h+\ell} a_i$ such that $c_i \neq \pm d_i$ holds for every $i = 1, 2, \ldots, t$. Let the deleted sequence be

$$Q\left(\prod_{i=1}^{t} c_i d_i\right)^{-1} = \prod_{i=1}^{p-h+\ell-2t} e_i.$$

By the Cauchy–Davenport theorem (Theorem 2.3), we infer that

$$\begin{aligned}\left|\sum(Q)\cup\{0\}\right| &\geqslant \sum_{i=1}^{t}|\{0,c_i,d_i,c_i+d_i\}| \\ &\quad+\sum_{i=1}^{p-h+\ell-2t}|\{0,e_i\}|-t-(p-h+\ell-2t)+1 \\ &=4t+2(p-h+\ell-2t)-t-(p-h+\ell-2t)+1 \\ &=p-h+\ell+t+1.\end{aligned}$$

Since $|\sum(Q)\backslash\{0\}|\leqslant p-h+720$, we have $t+\ell\leqslant 720$ and hence $t\leqslant 720$. Therefore, we get

$$p-h+\ell-2t\geqslant p-h-1440.$$

Also, by the maximality of t, we derive that

$$\prod_{i=1}^{p-h+\ell-2t} e_i=g^m(-g)^n$$

for some $g\in\mathbb{Z}_p\backslash\{0\}$, where $m\geqslant n\geqslant 0$ and $m+n=p-h+\ell-2t$. Since $n=p-h+\ell-2t-m$ and $m\leqslant h<\frac{2p}{5}$, we have

$$n\geqslant p-h-1440-\frac{2p}{5}>\frac{p}{5}-1440.$$

Set $w=\left[\frac{n}{2}\right]$ and form the zero subsequence $W=g^w(-g)^w$ of $\pi_1(S)$. Since $2w(n-w)>p$, the result follows from Theorem 2.4. $\square$

Lemma 3.7. *Let $p\geqslant 5.2\times 10^5$ be any prime number. Let $S=\prod_{i=1}^{p+Ol(\mathbb{Z}_p)-1}(a_i,b_i)$ be a subset of $\mathbb{Z}_p^2$. If $h=h(\pi_1(S))<p/360$ and $r+u+v\leqslant p/12$, then S contains a zero-sum subset.*

Proof. Consider the sequence

$$W=x_1^{m_1-2}x_2^{m_2-2}\cdots x_r^{m_r-2}y_1y_2\cdots y_uz_1z_2\cdots z_v$$

which is a subsequence of $\pi_1(S)$. Let R be the maximal zero subsequence of W. Then WR^{-1} is a zero-free sequence. If $|WR^{-1}|>p/4$, then by letting $k=361$ in Theorem 2.7 we get, $h(WR^{-1})\geqslant p/360$, a contradiction on $h(W)<p/360$. Therefore, $|WR^{-1}|<p/4$, and $|R|>|W|-p/4=p+d-1-2r-u-p/4$. Write $R=c_1^{l_1}c_2^{l_2}\cdots c_t^{l_t}c_{t+1}\cdots c_s$, where $c_1,c_2,\dots,c_s$ are pairwise distinct and $2\leqslant l_i\leqslant m_{j_i}-2$ for every $i=1,2,\dots,t$. Without loss of generality, we may assume that $j_i=i$ for $i=$

$1, 2, \ldots, t$. Note that

$$\begin{aligned}1+\sum_{i=1}^{t} l_i(m_i-l_i) &\geqslant 1+\sum_{i=1}^{t} 2(m_i-2)\\ &\geqslant 1+2(m_1+m_2+\cdots+m_t)-4t \geqslant 1+2(l_1+2+\cdots+l_t+2)-4t\\ &= 1+2(l_1+l_2+\cdots+l_t) = 1+2(|R|-s+t)\\ &\geqslant 1+2(p+d-1-2r-u-p/4-(s-t))\\ &\geqslant p+p+2d-1-4r-2u-2(r+u+v)-p/2)\\ &> p+p-6(r+u+v)-p/2\\ &\geqslant p+p-p/2-p/2 \geqslant p.\end{aligned}$$

Now, by Theorem 2.4 the result follows. □

Lemma 3.8. *Let $p>600$ be any prime number. Let $S=\prod_{i=1}^{p+Ol(\mathbb{Z}_p)-1}(a_i,b_i)$ be a subset of $\mathbb{Z}_p^2$. Let $k=[\sqrt{4p-7}]+1$. If $h(\pi_1(S))\geqslant k+1$ and $r+u+v\geqslant p/12$, then S contains a zero-sum subset.*

Proof. Since $p>600$, we have $r+u+v\geqslant p/12>k$. Without loss of generality, we may assume that $a_1, a_2, \ldots, a_k$ are pairwise distinct. Set $l=[k/2]$ and $A=\{a_1, a_2, \ldots, a_k\}$. By Theorem 2.2, we have $\sum_l(A)=\mathbb{Z}_p$. Since $h(\pi_1(S))\geqslant k+1$, the deleted sequence $\pi_1(S)A^{-1}$ contains some element a (say) with $v_a(\pi_1(S)A^{-1})\geqslant h-1\geqslant k$. Without loss of generality, we may assume that $a_{k+1}=a_{k+2}=\cdots=a_{k+h-1}=a$. Then the corresponding second co-ordinates $b_{k+1}, b_{k+2}, \ldots, b_{k+h-1}$ are pairwise distinct in $\mathbb{Z}_p$. Let $B=\{b_{k+1}, b_{k+2}, \ldots, b_{k+h-1}\}\subset\mathbb{Z}_p$. Then again by Theorem 2.2, we see that $\sum_l(B)=\mathbb{Z}_p$.

Let $\alpha=la$. Since $\sum_l(A)=\mathbb{Z}_p$, there is a subset $I\subset\{1,2,\ldots,k\}$ such that $\alpha+\sum_{i\in I}a_i=0$ and $|I|=l$. Let $\beta=\sum_{i\in I}b_i$. Now since $\sum_l(B)=\mathbb{Z}_p$, there is a subset $J\subset\{k+1,k+2,\ldots,k+h-1\}$ such that $\beta+\sum_{j\in J}b_j=0$ and $|J|=l$. Therefore,

$$\prod_{i\in I}(a_i,b_i)\prod_{j\in J}(a,b_j)$$

is a zero-sum subset of S. □

Theorem 3.9. *Let $p\geqslant 5\times 10^7$ be any prime. Let $S=\prod_{i=1}^{p+Ol(\mathbb{Z}_p)-1}(a_i,b_i)$ be a subset of $\mathbb{Z}_p^2$ of cardinality $p+Ol(\mathbb{Z}_p)-1$. Let $k=[\sqrt{4p-7}]+1$ be a positive integer. If $h=h(\pi_1(S))\geqslant k+1$, then S contains a zero-sum subset.*

Proof. Proof follows from Lemmas 3.2, 3.4, 3.5, 3.6, 3.7 and 3.8. □

Theorem 3.10. *Let M be a given positive integer. Let $p\geqslant(3M)^{6/7}$ be a prime number. Let $S\subset\mathbb{Z}_p^2$ be of cardinality $|S|=n$ such that $n\geqslant 3Mp^{5/6}$. Suppose that $|S\cap(H+$*

$x)|\leqslant M$ holds for all subgroups H of order p and all $x\in\mathbb{Z}_p^2$. Then S is not a zero-free subset.

Note: In the statement of Theorem 3.10, the assumption $n\geqslant 3Mp^{5/6}$ makes sense because as $p\geqslant(3M)^{6/7}$, we have $3Mp^{5/6}\leqslant p^2=|\mathbb{Z}_p\oplus\mathbb{Z}_p|$.

Proof. Put

$$f(\gamma)=\prod_{s\in S}(1+\gamma(s))=1+\sum_{x\in\sum(S)}n(x)\gamma(x),$$

where γ is any character of the group $\mathbb{Z}_p^2$, and the positive integer $n(x)$ stand for the number of times the element x is represented as a subset sum. If S is a zero-free subset, then we have

$$\sum_{\gamma}f(\gamma)=p^2.$$

Now this sum has a main term coming from the principal character γ_0 and which is 2^n. We estimate the other terms.

Suppose $\gamma\neq\gamma_0$. Values of γ are of the form $\exp(2\pi ij/p)$, and if $\gamma(s)=\exp(2\pi ij/p)$, then

$$|1+\gamma(s)|=2\cos\pi j/p.$$

If $|x|<\pi/2$, then $\cos x\leqslant\exp(-x^2/2)$ and so assuming $|j|<p/2$, we get

$$|1+\gamma(s)|\leqslant 2\exp(-c(j/p)^2)$$

with $c=\pi^2/2$.

Each value of j corresponds to a coset of a subgroup of order p. Thus it can occur for at most M values of s. Write

$$n=(2k-1)M+q,\ \ 0\leqslant q<2M.$$

We get the largest possible value of $|f(\gamma)|$ when j takes the values $0,1,-1,\dots,k-1,-(k-1)$ each M times and the remaining q values are split between k and $-k$. In this situation the above inequalities yield

$$|f(\gamma)|\leqslant 2^n\exp(-ct/p^2),$$

where

$$t=2M(1^2+2^2+\cdots+(k-1)^2)+qk^2.$$

A simple calculation gives

$$t\geqslant\frac{n(n^2-M^2)}{12M^2},$$

with equality when $q=0$. So we get

$$\sum_{\gamma}f(\gamma)\geqslant f(\gamma_0)-\sum_{\gamma\neq\gamma_0}|f(\gamma)|\geqslant 2^n(1-(p^2-1)\exp(-ct/p^2)).$$

Since $n \geqslant 3Mp^{5/6}$,

$$\exp(ct/p^2) > 2p^2,$$

and the above formula gives $\sum_\gamma f(\gamma) > 2^{n-1}$. By the choice of n, we have $n > 1 + (2/\log 2)\log p$ giving $\sum_\gamma f(\gamma) > p^2$, a contradiction. Hence the theorem. $\square$

Corollary 3.11. *Let $M = 10^5$ and a prime number $p > 4.67 \times 10^{34}$. Let $S \subset \mathbb{Z}_p^2$ be of cardinality $|S| = (p-1)/2$. Suppose that $|S \cap (H + x)| \leqslant M$ holds for all subgroups H of order p and all $x \in \mathbb{Z}_p^2$. Then S contains a zero-sum subset.*

Proof. Putting $M = 10^5$, $p > 4.67 \times 10^{34}$ and $n = (p-1)/2$ in Theorem 3.10 we get the result. $\square$

Theorem 3.12. *Let $p > 4.67 \times 10^{34}$ be any prime. Let $S = \prod_{i=1}^{p+Ol(\mathbb{Z}_p)-1}(a_i, b_i)$ be a subset of $\mathbb{Z}_p^2$ of cardinality $p + Ol(\mathbb{Z}_p) - 1$. Suppose that $|S \cap (H + x)| \leqslant k$ holds for all subgroups H of order p and all $x \in \mathbb{Z}_p^2$, where $k = [\sqrt{4p-7}] + 1$. Then S contains a zero-sum subset.*

Proof. Assume to the contrary that S is a zero-sum free set. Then $\phi(S)$ is zero-sum free set for every automorphism ϕ over $\mathbb{Z}_p^2$. Thus, we can choose a suitable automorphism ϕ such that the sequence $\pi_1(\phi(S))$ has minimal possible distinct elements of $\mathbb{Z}_p$. In other words, we can choose an automorphism ϕ such that $\phi(S)$ has the minimal possible value for $u + v + r$. For convenience, we denote $\phi(S)$ still by S. Set $d = Ol(\mathbb{Z}_p)$. Note that by the choice of p and hypothesis, we have $h(\pi_1(S)) < p/360$. Therefore, if $u + v + r < p/12$, then by Lemma 3.7, we can derive that S contains a zero-sum subset. So, we can assume that for any automorphism ϕ over $\mathbb{Z}_p^2$, we have

$$u + v + r \geqslant p/12.$$

Without loss of generality, we may assume that $a_1, a_2, \ldots, a_{[p/12]+1}$ are distinct. Let $A = \{a_1, a_2, \ldots, a_{[p/12]+1}\}$, $m = 3 \times 10^7$, and $v = \frac{m}{1500}$.

Let $t \geqslant 0$ be the largest integer such that there are tm disjoint subsets $I_1, I_2, \ldots, I_{tm}$ of $\{1, 2, \ldots, p + d - 1\}$ satisfying that,

(1) $|I_j| = v$ for every $j = 1, 2, \ldots, tm$.
(2) $\sum_{l \in I_j} a_l = 0$ for every $j = 1, 2, \ldots, tm$, and
(3) $\sum_{l \in I_{wm+1}} b_l, \sum_{l \in I_{wm+2}} b_l, \ldots, \sum_{l \in I_{wm+m}} b_l$ are pairwise distinct for every $w = 0, 1, \ldots, t-1$.

(If there is no disjoint subsets satisfying (1), (2) and (3) then set $t = 0$).

Let

$$B_w = \left\{ \sum_{l \in I_{wm+1}} b_l, \ \sum_{l \in I_{wm+2}} b_l, \ldots, \sum_{l \in I_{wm+m}} b_l \right\}$$

for every $w = 0, 1, \ldots, t-1$ and $n = m/2 = 15 \times 10^6$. By Theorem 2.1, we have

$$\left| \sum_n (B_w) \right| \geqslant n(|B_w| - n) + 1 = \frac{m^2+4}{4}$$

holds for every $w = 0, 1, \ldots, t-1$. Since S is zero-sum free set in $\mathbb{Z}_p^2$ (by our assumption), $B_0 B_1 \cdots B_{t-1}$ is a zero-sum free sequence in $\mathbb{Z}_p$ of length tm. Therefore, by Theorem 2.5, we derive that

$$\begin{aligned} t\frac{m^2+4}{4} &\leqslant \left| \sum_n (B_0) \right| + \left| \sum_n (B_1) \right| + \cdots + \left| \sum_n (B_{t-1}) \right| \\ &\leqslant \left| \sum (B_0) \right| + \left| \sum (B_1) \right| + \cdots + \left| \sum (B_{t-1}) \right| \\ &\leqslant \left| \sum (B_0 B_1 \cdots B_{t-1}) \right| < p. \end{aligned}$$

This implies

$$t < \frac{4p}{m^2+4}.$$

Let $T_1 = \pi_1(S)(\prod_{i \in K} a_i)^{-1}$ and $A_1 = A \backslash \mathrm{Supp}(\prod_{i \in K} a_i)$, where $K = \bigcup_{j=1}^{tm} I_j$. Then

$$|A_1| \geqslant |A| - |K| \geqslant \left[\frac{p}{12}\right] + 1 - vmt > \frac{p}{12} - \frac{4m^2 p}{1500(m^2+4)} > \frac{2p}{25} + v(m-1). \qquad (3)$$

Set $f_1 = |A_1|$. Without loss of generality, we may assume that

$$A_1 = \{a_1, a_2, \ldots, a_{f_1}\}$$

and hence $f_1 > \frac{2p}{25} + v(m-1)$. Hence by Theorem 2.1, we can get $|\sum_v (A_1)| = p$ which would imply there exists a subset I of $\{1, 2, \ldots, f_1\}$ of cardinality v such that $\sum_{i \in I} a_i = 0$ in $\mathbb{Z}_p$.

Let $w_1 \geqslant 1$ be the largest integer such that there are w_1 disjoint subsets $J_1, J_2, \ldots, J_{w_1}$ of T_1 satisfying the following conditions;

$(1)'$ $|J_l| = v$ for every $l = 1, 2, \ldots, w_1$;

$(2)'$ $\sum_{q \in J_l} a_q = 0$ for every $l = 1, 2, \ldots, w_1$, and

$(3)'$ $\sum_{l \in J_1} b_l, \ \sum_{l \in J_2} b_l, \ldots, \sum_{l \in J_{w_1}} b_l$ are pairwise distinct.

Set

$$B = \left\{ \sum_{l \in J_1} b_l, \sum_{l \in J_2} b_l, \ldots, \sum_{l \in J_{w_1}} b_l \right\}.$$

By the maximality of t, we see that $|B| = w_1 \leqslant m-1$. Let $T_2 = T_1(\prod_{i \in L} a_i)^{-1}$ and $A_2 = A_1 \backslash \mathrm{Supp}(\prod_{i \in L} a_i)$, where $L = \bigcup_{l=1}^{w_1} J_l$. Then

$$|A_2| \geqslant |A_1| - |L| \geqslant |A_1| - vw_1 > \frac{2p}{25}.$$

Without loss of generality, we may assume that

$$A_2 = \{a_1, a_2, \dots, a_{f_2}\}$$

and hence $f_2 > 2p/25$.

Let $E = \{1, 2, \dots, p+d-1\} \backslash (K \cup L)$. If $\mathscr{I}$ is a subset of E such that $|\mathscr{I}| = v$ and $\sum_{l \in \mathscr{I}} a_l = 0$, then by the maximality of w_1, we derive that

$$\sum_{l \in \mathscr{I}} b_l \in B.$$

Now, for every $g \in \mathbb{Z}_p$, we define

$$F_g = \left\{ \sum_{j \in O} b_j \colon\ O \subset E,\ |O| = \frac{v}{2},\ \sum_{j \in O} a_j = g \right\}.$$

We claim that

$$|F_g| \leqslant m-1 \text{ holds for every } g \in \mathbb{Z}_p. \tag{4}$$

Assume the contrary that $|F_g| \geqslant m$. Then there are m subsets $L_1, L_2, \dots, L_m$ (not necessary disjoint) of E such that $|L_i| = v/2$ with $\sum_{l \in L_i} a_l = g$ holds for every $i = 1, 2, \dots, m$ and such that $\sum_{l \in L_1} b_l, \sum_{l \in L_2} b_l, \dots, \sum_{l \in L_m} b_l$ are pairwise distinct. Since

$$\left| \{1, 2, \dots, f_2\} \Big\backslash \bigcup_{i=1}^{m} L_i \right| \geqslant \frac{2p}{25} - vm/2 > \frac{3p}{38},$$

by Theorem 2.1, there is a subset $\mathscr{J} \subset \{1, 2, \dots, f_2\} \backslash \bigcup_{i=1}^{m} L_i$ such that $|\mathscr{J}| = v/2$ and $\sum_{l \in \mathscr{J}} a_l = -g$. Hence $|\mathscr{J} \cup L_i| = v$ and $\sum_{l \in \mathscr{J} \cup L_i} a_l = 0$ for every $i = 1, 2, \dots, m$. Therefore, by the maximality of w_1, we have $\sum_{l \in \mathscr{J}} b_l + \sum_{l \in L_i} b_l \in B$ holds for every $i = 1, 2, \dots, m$. Since $|F_g| \geqslant m$, we see that $\sum_{l \in \mathscr{J}} b_l + \sum_{l \in L_i} b_l$ (for all $l = 1, 2, \dots, m$) are pairwise distinct. Therefore, $|B| \geqslant m$ which is a contradiction. This proves (4).

Now, let $S_2 = \prod_{i \in E} (a_i, b_i)$, then $T_2 = \pi_1(S_2)$. Set $t_2 = |T_2|$. Without loss of generality, we may assume that $T_2 = \prod_{i=1}^{t_2} a_i$. From (4), we derive that

$$\left| \left\{ \sigma(R) \colon\ R | S_2,\ |R| = \frac{v}{2} \right\} \right| \leqslant (m-1)p. \tag{5}$$

For any automorphism ϕ over $\mathbb{Z}_p^2$, we write $\phi(S_2) = \prod_{i=1}^{t_2} (a_i, b_i)$ (here we still write the elements of $\phi(S_2)$ by (a_i, b_i)). Write $T_2 = x_1^{k_1} \cdots x_\ell^{k_\ell}$ with $k_1 \geqslant k_2 \geqslant \cdots \geqslant k_\ell \geqslant 1$, $k_1 + k_2 + \cdots + k_\ell = t_2$ and $x_1, x_2, \dots, x_\ell$ are pairwise distinct. We distinguish two cases.

Case 1: (There is an automorphism ϕ over $\mathbb{Z}_p^2$ so that $k_1 > \frac{m}{300}$). In this case, $k_1 > 10^5$. Denote $\phi(S_2)$ still by S_2. First we shall prove that there is an element $g \in \mathbb{Z}_p$

such that

$$|K_g| \geqslant m, \tag{6}$$

where $K_g = \{\sum_{j\in O} b_j\colon\ O \subset \{1,2,\dots,t_2\},\ |O| = \frac{v}{4},\ \sum_{j\in O} a_j = g\}$.

We shall re-write S_2 as follows;

$$S_2 = \prod_{i=1}^{\ell} ((x_i, y_1^{(i)}) \cdots (x_i, y_{k_i}^{(i)})).$$

Let $g = \sigma(x_1^{600} x_2 \cdots x_{\frac{v}{4}-599}) = 600x_1 + x_2 + \cdots + x_{\frac{v}{4}-599}$.

Since S_2 is a subset of $\mathbb{Z}_p^2$, for every $i \in \{1,2,\dots,\ell\}$, we have $y_1^{(i)}, y_2^{(i)}, \dots, y_{k_i}^{(i)}$ are pairwise distinct in $\mathbb{Z}_p$. Set $M_i = \{y_1^{(i)}, y_2^{(i)}, \dots, y_{k_i}^{(i)}\}$ for every $i = 1,2,\dots,\ell$. Since $\ell = |\mathrm{Supp}(T_2)| \geqslant |A_2| > 2p/25 \geqslant \frac{v}{4} - 599$, by Theorem 2.1, we have

$$\begin{aligned}
|K_g| &\geqslant \left| \sum_{600} (M_1) + \sum_{1} (M_2) + \cdots + \sum_{1} (M_{\frac{v}{4}-599}) \right| \geqslant \left| \sum_{600} (M_1) \right| \\
&\geqslant 600(k_1 - 600) + 1 \\
&\geqslant 600\left(\frac{m}{300} - 600\right) + 1 > m
\end{aligned}$$

and this proves (6).

Now one can choose m subsets $J_1, J_2, \dots, J_m$ (not necessary disjoint) of $\{1,2,\dots,t_2\}$ such that $\sum_{j\in J_1} b_j, \sum_{j\in J_2} b_j, \dots, \sum_{j\in J_m} b_j$ are pairwise distinct with $|J_1| = \cdots = |J_m| = v/4$ and $\sum_{j\in J_1} a_j = \cdots = \sum_{j\in J_m} a_j = g$.

Let $U = \prod_{i=1}^{t_2} a_i (\prod_{j\in J_1\cup\cdots\cup J_m} a_j)^{-1}$. Then

$$\begin{aligned}
|\mathrm{Supp}(U)| &\geqslant |A_2| - |J_1 \cup \cdots \cup J_m| \\
&\geqslant \frac{2p}{25} - \frac{mv}{4} \\
&> \frac{3p}{38}.
\end{aligned}$$

Therefore, using Theorem 2.1, we arrive at

$$\sum_{v/4} (U) = \mathbb{Z}_p. \tag{7}$$

Let z_1 be an arbitrary element of $\mathbb{Z}_p$, then we can write $z_1 = g + g_1$ for some $g_1 \in \mathbb{Z}_p$. By (7), there exists $\kappa_1 \subset \{1,2,\dots,t_2\} \backslash \left(\bigcup_{i=1}^m J_i\right)$ such that $|\kappa| = v/4$ and $\sum_{i\in\kappa_1} a_i = g_1$. Therefore, we get $z_1 = \sum_{i\in\kappa_1} a_i + \sum_{j\in J_1} a_j = \cdots = \sum_{i\in\kappa_1} a_i + \sum_{j\in J_m} a_j$ and such that the sums of their corresponding second co-ordinates $\sum_{i\in\kappa_1} b_i + \sum_{j\in J_1} b_j, \dots, \sum_{i\in\kappa_1} b_i + \sum_{j\in J_m} b_j$ are pairwise distinct. Therefore, in this case we get

$|F_{z_1}| \geqslant m$. As z_1 is arbitrary, we have $|F_z| \geqslant m$ for every $z \in \mathbb{Z}_p$ and hence, we get

$$\left|\left\{\sigma(R)\colon\ R|S_2,\ |R| = \frac{v}{2}\right\}\right| \geqslant mp,$$

which contradicts (5). Hence in this case, S cannot be a zero-sum free set.

Case 2: (For every automorphism ϕ over $\mathbb{Z}_p^2$ we always have $k_1 \leqslant \frac{m}{300} = 10^5$). Clearly, $|S_2| = |E| = p + d - 1 - |K \cup L| \geqslant p + d - 1 - |K| - |L|$. By (3), we know that $[p/12] + 1 - vmt > 2p/25 + v(m-1)$. Therefore, we have

$$|K| + |L| \leqslant vmt + v(m-1) < \left[\frac{p}{12}\right] + 1 - \frac{2p}{25} \leqslant \frac{p}{300} + 1.$$

Hence,

$$|S_2| \geqslant p + d - 1 - \frac{p}{300} - 1 \geqslant \frac{p-1}{2}.$$

Since $p > 4.67 \times 10^{34}$ and conditions of Corollary 3.11 are satisfied, we see that S_2 and therefore S cannot be a zero-sum free set. Hence the theorem. $\square$

Proof of Theorem 1.1. Let $p > 4.67 \times 10^{34}$ be any prime number. Let S be a subset of $\mathbb{Z}_p^2$ of cardinality $p - 1 + Ol(\mathbb{Z}_p)$. Set $k = [\sqrt{4p-7}] + 1$. If there is an automorphism ϕ over $\mathbb{Z}_p^2$ such that the first co-ordinate sequence of $\phi(S)$ contains some element at least $k+1$ times, then the main theorem follows from Theorem 3.9. Otherwise, $|S \cap (H + x)| \leqslant k$ holds for all subgroups H of order p and all $x \in \mathbb{Z}_p^2$. Then by Theorem 3.12, S contains a zero subsequence. $\square$

Acknowledgments

The first author is partially supported by an NSFC Grant 10271080 and an MOEC Grant 02047. We are thankful to referees for their very useful comments.

References

[2] N. Alon, M.B. Nathanson, I.Z. Ruzsa, The polynomial method and restricted sums of congruence classes, J. Number Theory 56 (2) (1996) 404–417.
[3] J.D. Bovey, P. Erdős, I. Niven, Conditions for zero-sum modulo n, Canad. Math. Bull. 18 (1) (1975) 27–29.
[4] A.L. Cauchy, Recherches sur les nombers, J. École Polytech. 16 (9) (1813) 99–123.
[5] H. Davenport, On the addition of residue classes, J. London Math. Soc. 10 (1935) 30–32.
[6] J.A. Dias da Silva, Y.O. Hamidoune, Cyclic spaces for Grassmann derivatives and additive theory, Bull. London Math. Soc. 26 (2) (1994) 140–146.
[7] P. Erdős, R.L. Graham, Old and new problems and results in combinatorial number theory, L' Enseignement Mathématique, Universitè de Geneve, Vol. 28, Genève, 1980.
[8] P. Erdős, H. Heilbronn, On the addition of residue classes mod p, Acta Arith. 9 (1964) 149–159.

[9] W.D. Gao, A. Geroldinger, On the structure of zero-free sequences, Combinatorica 18 (4) (1998) 519–527.
[10] W.D. Gao, A. Geroldinger, On long minimal zero sequences in finite abelian groups, Period. Math. Hungar. 38 (3) (1999) 179–211.
[11] Y.O. Hamidoune, G. Zémor, On zero-free subset sums, Acta Arith. 78 (2) (1996) 143–152.
[12] C. Julio, J. Subocz, Some values of Olson's constant, Divulg. Mat. 8 (2) (2000) 121–128.
[13] J.E. Olson, An addition theorem modulo p, J. Combin. Theory 5 (1968) 45–52.
[14] J.E. Olson, Sum of sets of group elements, Acta Arith. 28 (2) (1975/76) 147–156.
[15] P. Scherk, Distinct elements in a set of sums, Amer. Math. Monthly 62 (1955) 46–47.
[16] E. Szemerédi, On a conjecture of Erdős and Heilbronn, Acta Arith. 17 (1970) 227–229.